

INFORME COMITÉ DE AUDITORÍA EJERCICIO 2023

En cumplimiento de lo señalado por la Superintendencia Financiera de Colombia (en adelante, “SFC”) en la Circular Básica Jurídica - CBJ (6.1.2. del Capítulo IV del Título I Parte I) la Junta Directiva de Banco Bilbao Vizcaya Argentaria Colombia S.A. (en adelante “BBVA Colombia”, o la “Entidad” o el “Banco”) cuenta con el Comité de Auditoría (en adelante el “Comité”), órgano de estudio y apoyo que le asiste en el cumplimiento de su función de supervisión de la Arquitectura de Control de la Entidad, que aborda todo lo relacionado con ambiente de control, gestión de riesgos, sistema de control interno, comunicación y monitoreo.

La regulación del Comité de Auditoría se encuentra establecida en la Ley 964 de 2005, en la citada Circular de la SFC, en el Reglamento de la Junta Directiva artículo 13.1 y en el Reglamento Interno que regula, en concordancia con las mencionadas normas, su naturaleza, objeto, composición, funciones, reuniones y demás aspectos relacionados con su funcionamiento, documentos que se encuentran publicados en la página Web del Banco www.bbva.com.co.

▪ Composición

El Comité está conformado por tres Directores de la Junta Directiva, que tienen la calidad de independientes y es presidido por uno de ellos. Cada uno de los miembros del Comité cuenta con la experiencia y conocimiento suficiente para el cumplimiento de las funciones que corresponden al mismo.

Durante el ejercicio 2023, el Comité estuvo conformado como se indica a continuación:

Director	Cargo	Condición	Nombramiento como miembro del Comité
Carlos Caballero Arguez	Presidente	Independiente	17.03.2005
Camila Escobar Corredor	Vocal	Independiente	26.03.2021
Luis Julián Martín Carranza Ugarte	Vocal	Independiente	27.04.2022

Los perfiles de cada miembro del Comité pueden consultarse en la página web <https://www.bbva.com.co/personas/atencion-al-inversionista/gobierno-corporativo/comite-de-apoyo.html>.

2. Funcionamiento

El Comité de Auditoría, conforme lo señalado en la Circular Básica Jurídica – CBJ de la SFC, la Ley 964 de 2005 (Artículo 45 Parágrafo 4º) sesiona trimestralmente, y sus decisiones y actuaciones quedan consignadas en actas firmadas por el Presidente y el Secretario del Comité, en cumplimiento de los requisitos establecidos en el art. 189 del Código de Comercio.

El Comité desempeña sus funciones con autonomía de funcionamiento y está dirigido por su Presidente, quien con objeto de favorecer una diversidad de opiniones que enriquezca los análisis y las propuestas del Comité, vela por la participación de los todos sus integrantes con libertad en las deliberaciones y fomentando el diálogo constructivo, promoviendo la libre expresión de sus opiniones.

Adicionalmente, el Comité cuenta con la presentación de informes por parte de la Revisoría Fiscal, Auditoría Interna y el Oficial de Cumplimiento, así como también cuenta con informes por parte de los miembros de la Alta Gerencia, cuando se considere necesario para el cumplimiento de sus funciones.

De conformidad con lo establecido en el Reglamento Interno del Comité, este puede acudir a servicios externos de asesoramiento en asuntos relevantes cuando considere que, por razones de especialización o independencia, no puedan éstos prestarse por expertos o técnicos del Banco.

En el ejercicio 2023 el Comité de Auditoría se reunió cinco veces, habiendo participado en las sesiones celebradas la totalidad de sus miembros. Igualmente, en las sesiones participó la Firma de Revisoría Fiscal Ernst & Young SAS- EY, y los máximos ejecutivos de las áreas de Auditoría Interna y de Control Interno y Cumplimiento.

3. Objeto

El objeto del Comité es brindar apoyo en la supervisión de los estados financieros, cumplimiento de los planes anuales de la Revisoría Fiscal, Auditoría Interna y del Área de Cumplimiento, y la gestión que realiza la Junta Directiva del Banco respecto de la implementación y supervisión de la Arquitectura de Control.

Adicionalmente, es tarea del Comité asegurar que la Entidad esté cumpliendo las leyes y regulaciones pertinentes y que en los negocios se mantengan los controles efectivos frente a los conflictos de interés y el fraude.

A través del Comité de Auditoría se asegura que la Entidad suministre la información requerida, y que para el desarrollo de sus funciones la Revisoría Fiscal, la Auditoría Interna y el Oficial de Cumplimiento, cuenten con los medios adecuados tanto en lo que se refiere al personal, como a elementos materiales, herramientas tecnológicas, procedimientos y manuales de actuación.

El detalle de las funciones del Comité de Auditoría se encuentran en el numeral 4° del Reglamento Interno respectivo, que puede ser consultado en la página web del Banco.

4. Actividades más relevantes desarrolladas por el Comité de Auditoría:

Durante el ejercicio 2023 el Comité desempeñó sus funciones con autonomía de funcionamiento, cumpliendo con el cronograma de sesiones y el orden del día que fue coordinado por su Presidente junto con el Secretario General del Banco.

En el ejercicio evaluado, el Comité se reunió cinco (5) veces (febrero, abril, mayo, agosto y noviembre) con asistencia del 100% de sus integrantes, contó con la participación de la Revisoría Fiscal, el Oficial de Cumplimiento y el Auditor Interno, entre otros, asegurando y manteniendo una línea de comunicación permanente de esta instancia con la Junta Directiva y la Administración del Banco.

El Comité realizó todas las actividades necesarias para dar cumplimiento a las funciones asignadas por la regulación vigente, los Estatutos Sociales y su Reglamento Interno.

Dentro de las principales actividades que desarrolló el Comité, se destacan:

a) Presentación y divulgación de la información financiera:

- El Comité estudió y emitió su opinión sobre los Estados Financieros separados y consolidados, tanto intermedios como anuales correspondientes al ejercicio 2023, en el sentido de que éstos cumplen en cuanto a su contenido y su forma, con todos los requisitos establecidos al respecto por la regulación y que han sido elaboradas siguiendo las mejores prácticas y recomendaciones, nacionales e internacionales en esta materia y en la legislación vigente.*

- *El Comité emitió opinión favorable para la presentación de los Estados Financieros separados y consolidados a consideración de la Asamblea General de Accionistas, a través de la Junta Directiva, manifestando que cumplen en cuanto a su contenido y forma con los requisitos y recomendaciones establecidas por la regulación y que han sido elaborados siguiendo las políticas y criterios contables que resultan de su aplicación.*

b) Respecto del Sistema de Control Interno

El Comité de Auditoría ha supervisado y conocido los distintos informes elaborados, tanto internamente como por el Revisor Fiscal sobre el Sistema de Control Interno de BBVA Colombia y sus filiales, estableciendo que el SCI proporciona seguridad razonable en la búsqueda de los siguientes objetivos:

- *Efectividad y eficiencia de las operaciones, esto es, el cumplimiento de los objetivos básicos de la Entidad, salvaguardando los recursos de la misma;*
- *Suficiencia y confiabilidad de la información financiera así como de la preparación de todos los Estados Financieros.*
- *Cumplimiento de la regulación aplicable.*
- *Contar con una estructura organizacional documentada, con divisiones de responsabilidades, políticas y procedimientos.*

Igualmente, durante el año 2023, el Comité ha realizado seguimiento al cumplimiento de las instrucciones dadas por la Junta Directiva en relación con el SCI.

c) Respecto de la Revisoría Fiscal:

La Asamblea General Ordinaria de Accionistas en sesión del dieciséis (16) de marzo de 2022 se eligió a Ernst & Young S.A.S. como Revisor Fiscal para los ejercicios 2022 y 2023, suministrando al Comité información directa en todas las sesiones.

El Comité ha conocido y dado su conformidad al Plan de Trabajo del ejercicio 2023 de la Revisoría Fiscal, teniendo en cuenta los asuntos clave y evaluación de riesgos, manteniendo comunicación continua con la Administración del Banco y conservando la independencia como corresponde. A su vez, ha seguido el grado de avance del desarrollo de su actividad, las recomendaciones formuladas respecto de sus hallazgos y los planes adoptados por la Entidad para su implementación.

En relación con la realización de los trabajos de auditoría y de acuerdo al plan de trabajo de 2023, el Comité ha sido informado y ha analizado, entre otros aspectos, lo siguiente:

- *Aprobación del Plan de trabajo y actualizaciones de los compromisos trimestrales*
- *Seguimiento de la actividad del Plan*
- *Conclusiones más relevantes de los trabajos realizados*
- *Seguimiento de recomendaciones*

Adicionalmente, el Comité ha supervisado los servicios de la Revisoría Fiscal durante todo el ejercicio, verificando que estos fueron ejecutados con calidad, independencia, desempeño y efectividad, considerándolo un aliado para los órganos de gobierno y dirección en su función de supervisión y evaluación de la eficacia del Control Interno y de los Sistemas de Gestión de Riesgo y Cumplimiento.

d) Respecto de la Auditoría Interna:

El plan de trabajo de Auditoría Interna se determina en una referencia trienal que se actualiza anualmente. La visión anual se concreta en planes trimestrales que resultan de un proceso de priorización que Auditoría Interna realiza cada trimestre. Para la definición de estos planes, se lleva

a cabo un risk assessment (RA) continuo que analiza el nivel de riesgo y el grado de control de la actividad desarrollada por cada sociedad del Grupo. El resultado del RA se materializa en las ceremonias de priorización anuales, que facilitan la conformación de la referencia trienal, y en las ceremonias de priorización trimestrales, en las cuales se determina qué trabajos se van a iniciar y se establece un compromiso sobre el número de trabajos que se van a emitir en el siguiente trimestre.

En las priorizaciones trimestrales, además del resultado del RA continuo, se tienen en cuenta los compromisos y expectativas de los supervisores, los objetivos estratégicos del Grupo, las líneas estratégicas de Auditoría Interna y las peticiones recibidas de las unidades. El análisis de riesgos y los planes trimestrales de 2023 se han estructurado por primera vez en torno a la taxonomía de riesgos corporativa del Grupo BBVA, constituida por veinte riesgos.

El Plan de Auditoría Interna 2023 contó con ceremonias trimestrales de priorización, así como la integración de trabajos Intra Q (no planificados), donde los audit partners fueron responsables de valorar las necesidades presentadas por parte de la administración y el regulador. De igual manera, los trabajos de assurance 2023 han dado cumplimiento al arquetipo Agile definido por el departamento de Auditoría como parte del apoyo brindado por el equipo de Auditoría Interna a la estrategia del Banco y sus filiales.

A continuación se presentan las actividades que, al arrojar resultados significativos, fueron objeto de seguimiento por parte de la Alta Dirección y del Comité de Auditoría.

- **Riesgo de gestión del dato.** Hace referencia a que los datos de la entidad no están organizados de manera práctica y utilizable, por lo que no se garantiza que todo el cuerpo de datos de la entidad sea preciso, coherente, de fácil acceso y que esté protegido adecuadamente.

En 2023 el área desarrolló el trabajo de Herramientas de Monitoreo Transaccional, en el que observó la necesidad de trabajar para robustecer el sistema de monitoreo de transacciones con el fin de garantizar una adecuada prevención y detección del fraude, así como desarrollar una gestión proactiva para reducir los niveles de fraude.

De igual manera, se llevó a cabo la evaluación del cálculo del Liquidity Coverage Ratio (LCR), en el que se observó que deben ejecutarse mejoras en las estimaciones de las “salidas de liquidez” que, si bien disminuyen el ratio, no supondrían un incumplimiento del límite de gestión establecido, ni tendrían impacto en el reporting consolidado. Además, es necesario adecuar los criterios y controles aplicados en el cálculo de las estimaciones, concretamente en la segmentación de clientes y la determinación de depósitos minoristas y operativos.

- **Riesgo de procesamiento transaccional.** Es el riesgo de pérdida resultante de un fallo o una falta de adecuación de los procesos, el personal, los sistemas internos o de acontecimientos externos. El trabajo de Valoración y Registro de Operaciones de Global Markets permitió establecer la necesidad de reforzar el marco de gobierno para garantizar la trazabilidad de las operaciones y establecer mejoras alrededor de la autorización de operaciones anuladas, modificadas y predatadas en los aplicativos Murex y Star.
- **Riesgo de modelo de negocio.** Se refiere al impacto en la capacidad de generar beneficios en escenarios adversos como consecuencia de factores internos (por ejemplo, pricing erróneo, objetivos inadecuados o fallos en la implementación de la estrategia) y externos (por ejemplo,

cambios en el entorno macro o en la competencia).

Como parte de las actividades alineadas con la estrategia, se desarrolló la actividad Comercialización y Gestión de Tarjetas de Crédito, siendo necesario un ajuste en la gestión de ventas improductivas, anticipación ante posibles deterioros en el producto y seguimiento a la puesta del producto en manos del cliente. De igual manera, el área desarrolló la revisión al Nuevo Modelo de Oficinas (NMO), identificando la necesidad de monitorear transacciones que no cuentan con una segregación funcional adecuada, así como considerar actividades que impactan la carga operativa, no tenidas en cuenta en el análisis inicial del proyecto.

- **Riesgo tecnológico.** Se define como la posibilidad de que el Banco sufra impactos negativos financieros, de negocio o en el capital o en la reputación, derivados de la tecnología de información y del procesamiento inadecuado, en términos de disponibilidad, integridad, autenticidad y confidencialidad.

La actividad finalizada en 2023 correspondiente a software security assurance permitió identificar la necesidad de reforzar los controles que garanticen las pruebas de seguridad previo paso a producción, así como el establecimiento de una metodología de desarrollo seguro.

- **Riesgo de seguridad de la información.** Asociado con el potencial de que las amenazas exploten la vulnerabilidad de un activo de información o grupo de activos de información y, por lo tanto, causen daños a la entidad. Alineados con la estrategia del Grupo en Colombia, el área realizó el aseguramiento de la herramienta Global Mobile App (GloMo), observando debilidades respecto de la identificación de fraudes bajo modalidades como vishing. Así mismo, se identificó la necesidad de robustecer actividades relacionadas con la continuidad del servicio y la detección de vulnerabilidades.

Para cada una de estas actividades, la administración estableció planes de acción con el fin de mitigar los riesgos identificados. Estos planes son objeto de seguimiento por parte de Auditoría Interna y, al cierre de 2023, no se observaron acciones vencidas según la metodología establecida.

Los Sistemas de Administración de Riesgo (Sistema Integral de Administración de Riesgos - SIAR, Sistema de Atención al Consumidor - SAC y Sistema de Administración de Riesgo de Lavado de Activos y Financiación del Terrorismo - SARLAFT), fueron evaluados atendiendo la normativa y la periodicidad definida por el regulador, llamando la atención sobre el SAC, en el cual el área observó las necesidades de alinear algunos aspectos establecidos con la entrada de la herramienta de la Superintendencia Financiera de Colombia, Smartsupervision.

De igual manera, en 2023 se llevaron a cabo revisiones sobre el resto de riesgos asociados a la nueva taxonomía, sin que se identificaran situaciones adicionales a las comentadas al Comité de Auditoría o a los órganos de vigilancia y control.

El seguimiento de acciones de AI constituye un punto de interés prioritario para los órganos de gobierno, la dirección del Grupo y para los principales organismos supervisores. El alto grado de concienciación e implicación de la dirección del Grupo BBVA en la implantación de recomendaciones y las medidas encaminadas a hacer un seguimiento proactivo por parte de Auditoría Interna, tuvieron un impacto positivo que se aprecia en la disminución de recomendaciones de los últimos años.

Por último, Auditoría Interna cuenta con un Programa de Aseguramiento y Mejora de la Calidad (PAMC) que cubre todas las actividades que desarrolla. Este modelo ha sido diseñado para garantizar que el área realice su trabajo conforme a las Normas Internacionales de Auditoría Interna y se cumpla la metodología interna.

e) *Respecto de Cumplimiento*

El Comité realizó seguimiento a los asuntos más relevantes presentados por la Oficial de Cumplimiento en línea con lo establecido en la Circular Básica Jurídica, revisando los informes correspondientes a la gestión, evaluación y control del Sistema de Administración del Riesgo de Lavado de Activo y de Financiación del Terrorismo -SARLAFT, seguimiento a la eficacia de los canales de denuncia y a las actuaciones de los miembros de la Junta Directiva relativas al Reglamento de la Junta Directiva, en el mercado de valores y el cumplimiento de Código de Conducta.

f) *Respecto de autoridades de supervisión:*

El Comité ha tenido conocimiento de las comunicaciones remitidas al Banco por parte de las Autoridades de supervisión, como la Superintendencia Financiera de Colombia, realizando seguimiento de los asuntos que dieron lugar a tales comunicaciones, las respuestas dadas a las autoridades y los planes de acción para llevar a cabo los requerimientos recibidos.

5. Deficiencias materiales detectadas, recomendaciones formuladas y medidas adoptadas:

No se presentaron deficiencias materiales

6. Observaciones formuladas por órganos de supervisión:

Superintendencia Financiera de Colombia (SFC):

Orden Administrativa Reporte de Formatos e Información requerida por la SFC y otras autoridades judiciales y administrativas

Hallazgo: Debilidades en los sistemas de Información Gerencial: i) En los procesos de elaboración, validación, calidad, consistencia, reporte y transmisión de los formatos. ii) En la oportunidad de atención de solicitudes de información formuladas por la SFC y otras autoridades. Orden Administrativa:

1. **SUSPENDER LAS SIGUIENTES PRÁCTICAS:** i) No atender las instrucciones de la SFC, de manera oportuna, con calidad, completitud y suficiencia de información y/o sin los requisitos formales establecidos en los instructivos para el diligenciamiento de formatos; ii) No suministrar la información que debe ser entregada al público, atendiendo requisitos e instructivos de los formatos; iii) No atender oportuna y completamente las comunicaciones de la SFC y otras autoridades. 2. Lectura del Requerimiento ante la Junta Directiva y remisión del extracto de acta 5 días hábiles siguientes a la sesión.

2. **DIAGNÓSTICO INTEGRAL:** Identificar la causa raíz de las fallas recurrentes en generación, validación y reporte de información a la SFC, así como en la atención de oficios de la SFC y de otras autoridades administrativas o judiciales. En el diagnóstico debe participar el área encargada de la gestión de riesgos y debe ser aprobado por un representante legal.

3. **DISEÑAR Y EJECUTAR UN PLAN DE ACCIÓN:** i) Adoptar medidas que den solución efectiva a los inconvenientes identificados en los procesos de elaboración, validación y transmisión de formatos, como en la atención de requerimientos, con calidad y en los plazos definidos. ii) El plan

debe incluir actividades, fechas de ejecución, áreas involucradas y responsables tanto de cada etapa como del plan en general. iii) El plan debe ser aprobado por la Junta Directiva y formar parte de las actividades y seguimiento de la Auditoría Interna. Plazo para la implementación del plan: 8 meses (febrero de 2024). iv) Enviar avance del cumplimiento de las etapas del plan de acción a la SFC firmado por representante legal: los 5 primeros días de cada mes hasta implementar el plan. v) La Auditoría Interna debe remitir certificación sobre la efectividad de las medidas una vez se concluya el plan de acción.

Nuevo requerimiento: La SFC requiere aclarar información remitida por el banco en tema de formatos; así como la efectividad del plan de acción propuesto respecto de las Investigaciones por LAFT y delitos contra la Administración Pública y Medidas Cautelares; iii) Seguimiento a la Auditoría Interna – AI: Solicita el pronunciamiento de la SFC sobre el cumplimiento de cada etapa del plan de acción; y iv) Se requiere el pronunciamiento de la Junta sobre el seguimiento al plan de acción según lo indicado en las Actas 1717 (26 de julio) y 1719 (27 de septiembre) de 2023; Se remitió respuesta, en espera de pronunciamiento de la SFC

Instrucción – Habilitar Canales Virtuales para el pago total o parcial de obligaciones

La SFC realizó seguimiento a través de una mesa de trabajo, en la cual se informaron los avances del proceso y se ratificó que consumo estará habilitado para marzo de 2023, pero se acordó que en la medida que avance el proyecto se revisará si se puede disminuir los tiempos, en especial respecto de los otros productos.

Desmaterialización de pagarés:

Requerimiento: i) completar encuesta sobre responsables de remitir el estado de la desmaterialización de pagarés y razón de cobertura; ii) Estructura del reporte que se debe remitir a corte de 31/oct; 30 Nov.; 31.Dic./2023. Posteriormente el reporte será mensual dentro de los 5 días hábiles siguientes a la transmisión de los EEFF del respectivo corte; iii) Evaluación de riesgos para la desmaterialización de pagarés en el IIS/2023; iv) Informe de resultados de la Auditoría Interna, incluyendo el estado de la medida correctora cuya finalización se programó para Dic. 2023.

Plan de Resolución –PR

La SFC expidió la Circular Externa 027 de 2019, mediante la cual impartió instrucciones sobre la forma de elaborar y presentar lo PR, además de definir los criterios para seleccionar a las entidades vigiladas. Adicionalmente, señaló la metodología para determinar las entidades con importancia sistémica, considerando categorías como tamaño, interconexión, sustitubilidad y complejidad. El Banco remitió el plan de Resolución con los ajustes y respuesta a las inquietudes planteadas por la SFC, en espera de pronunciamiento.

Sanciones

Mediante Resolución del 9 de octubre de 2023, la Dirección de Investigaciones de Protección de Datos Personales de la Superintendencia de Industria y Comercio (SIC) resolvió la actuación administrativa sancionatoria, declarando que BBVA Colombia no informó debidamente la finalidad de la recolección de datos personales y los derechos que le asistían como titular, en contravía con los literales b) y c) del artículo 17 de la Ley 1581 de 2012, en concordancia con los literales b) y c) del artículo 4 y el artículo 12 de esa misma Ley, y los artículos 2.2.2.25.2.2. y 2.2.2.25.2.5. del Decreto 1074 de 2015.

Se impuso una multa a BBVA Colombia por COP 339,3 millones y se emitió una orden administrativa consistente en que el Banco “implemente un procedimiento para solicitar la autorización del tratamiento de datos personales de los referidos, si el tratamiento de dichos datos se va a realizar con motivos diferentes a los de verificar la identidad del solicitante en el momento en que este celebre



Creando Oportunidades

un negocio jurídico con el Banco. Dicha autorización deberá respetar los requisitos establecidos en la Ley 1581 de 2012 y sus Decretos Reglamentarios". Para este fin se concedieron 3 meses contados desde la ejecutoria de la Resolución, para lo cual se debería remitir una certificación suscrita por el representante legal de BBVA Colombia. El Banco interpuso los recursos de ley.

7. Evaluación de la labor realizada por la Auditoría Interna:

El Comité supervisó las funciones y actividades de la Auditoría Interna pudiendo determinar su independencia y objetividad en relación con las actividades que audita, indicando que no existieron limitaciones que impidieran su adecuado desempeño y que el alcance de su labor cumplió las necesidades de la Entidad.